AMENDMENT

Please amend the application as indicated hereafter.

In The Claims:

Claim 1. (currently amended) A system for detecting an illegal loading of a software with a software serial number and executing the software thereafter, the system comprising:

a personal identity circuit for generating an inspection code with [[an]] a first value corresponding to a software when the software is installed in the system at the first time and a software serial number of the software is received by the personal identity circuit, wherein if ~~the inspection code corresponding to the software is not generated~~ the personal identity circuit is not present, the execution of the software is terminated; and

a communication control interface having a communication equipment serial number, the communication control interface [[is]] being provided for connecting the personal identity circuit with a new product registration center, wherein the new product registration center receives the software serial number and the communication equipment serial number and compares the software serial number and the communication equipment serial number with datasets in a database in the new product registration center, wherein when the software serial number is found within one of the datasets but a communication equipment serial number in the one of the datasets differs from the received communication equipment serial number, the inspection code is reset to [[an]] a second value, wherein the first value indicates the installed software is in a legal user state and the second value indicates the installed software is in an illegal user state,

wherein the software automatically checks the inspection code before executing the

software, when the inspection code is in the legal user state, executing of the software permitted, when the inspection code is in the illegal user state, executing of the software is terminated immediately.

Claim 2. (currently amended) The system of claim 1, wherein when both of [[he]] the received software serial number and the received communication equipment serial number are not found among the datasets, the software serial number and the communication equipment serial number are written down as a new dataset in the database and then the inspection code is reset to the legal user state.

Claim 3. (original) The system of claim 2, wherein the new product registration center is connected to a software manufacturer system for reporting a software registration to the software manufacturer system after the new product registration center reset the inspection code to the legal user state according to the software serial number and the communication equipment serial number.

Claim 4. (canceled)

Claim 5. (original) The system of claim 1, wherein the communication control interface comprises a network interface card.

Claim 6. (original) The system of claim 1, wherein the communication control interface comprises a wireless communication network.

Claim 7. (original) The system of claim 1, wherein the communication control interface comprises a global positioning system.

Claim 8. (original) The system of claim 1, wherein the new product registration center is connected to a software manufacturer system for reporting a software registration to the software manufacturer system after the new product registration center reset the inspection code to the legal user state according to the software serial number and the communication equipment serial number.

Claim 9. (original) The system of claim 1, wherein the personal identity circuit further comprises:

a microprocessor having a memory unit for generating the inspection code when installing the software;

a non-volatile memory unit coupled to the microprocessor for holding the inspection code; and

a media access controller coupled to the non-volatile memory unit and the communication control interface for transmitting the inspection code to the new product registration center via the communication control interface.

Claim 10. (original) The system of claim 9, wherein the memory unit comprises an erasable programmable read-only-memory.

Claim 11. (original) They system of claim 9, wherein the memory unit comprises an electrically erasable programmable read-only-memory.

Claim 12. (original) The system of claim 9, wherein the memory unit comprises a flash memory.

Claim 13. (original) The system of claim 9, wherein the memory unit comprises a static random access memory.

Claim 14. (original) The system of claim 9, wherein the memory unit comprises a dynamic random access memory.

Claim 15. (original) The system of claim 9, wherein the non-volatile memory unit comprises an erasable programmable read-only-memory.

Claim 16. (original) The system of claim 9, wherein the non-volatile memory unit comprises an electrically erasable read-only-memory.

Claim 17. (original) The system of claim 9, wherein the non-volatile memory comprises a flash memory.

Claim 18. (original) The system of claim 1, wherein the personal identity circuit further comprises:

a microprocessor having a memory unit for generating the inspection code when installing the software;

a non-volatile memory unit coupled to the microprocessor for holding the inspection code; and

a media access controller coupled to the non-volatile memory unit and the

communication control interface for transmitting the inspection code to the new product registration center via the communication control interface.

Claim 19. (currently amended) A chip in a system for detecting an illegal loading of a software with a software serial number and executing the software thereafter, the chip comprising:

a microprocessor for generating an inspection code with [[an]] a first value corresponding to a software when the software is installed in the system at the first time and a software serial number of the software is received by the microprocessor, wherein if ~~the inspection code corresponding to the software is not generated~~ the microprocessor is not present, the execution of the software is terminated;

a non-volatile memory unit coupled to the microprocessor for holding the inspection code; and

a media access controller coupled to the non-volatile memory unit and a communication control interface for transmitting the software serial number of the software and a communication equipment serial number to a new product registration center via the communication control interface, wherein the new product registration center receives the software serial number and the communication equipment serial number and compares the software serial number and the communication equipment serial number with datasets in a database in the new product registration center, wherein when the software serial number is found within one of the datasets but a communication equipment serial number in the one of the datasets differs from the received communication equipment serial number, the inspection code

is reset to [[an]] a second value, wherein the first value indicates the installed software is in a legal user state and the second value indicates the installed software is in an illegal user state,

wherein the software automatically checks the inspection code before executing the software, when the inspection code is in the legal user state, executing of the software is permitted, when the inspection code is in the illegal user state, executing of the software is terminated immediately.

Claim 20. (original) The chip of claim 19, wherein the communication control interface comprises a network interface card.

Claim 21. (original) The chip of claim 19, wherein the communication control interface comprises a wireless communication network.

Claim 22. (original) The chip of claim 19, wherein the communication control interface comprises a global positioning system.

Claim 23. (original) The chip of claim 19, wherein the non-volatile memory unit comprises an erasable programmable read-only-memory.

Claim 24. (original) They chip of claim 19, wherein the non-volatile memory unit comprises an electrically erasable programmable read-only-memory.

Claim 25. (original) The chip of claim 19, wherein the non-volatile memory unit comprises a flash memory.

Claim 26. (currently amended) A method of using hardware to detect an illegal loading of a software with a software serial number and executing the software thereafter, the method comprising:

generating an inspection code with [[an]] a first value corresponding to a software by a personal identity circuit when the software is installed at the first time and a software serial number of the software is received, wherein ~~the inspection code corresponding to the software is not generated~~ the personal identity circuit is not present, the execution of the software is terminated,

and

transmitting the software serial number and a communication equipment serial number of the computer to a new product registration center;

wherein the new product registration center receives the software serial number and the communication equipment serial number and compares the software serial number and the communication equipment serial number with datasets in a database in the new product registration center, wherein when the software serial number is found within one of the datasets but a communication equipment serial number in the one of the datasets differs from the received communication equipment serial number, the inspection code is reset to [[an]] a second value, wherein the first value indicates the installed software is in a legal user state and the second value indicates the installed software is in an illegal user state,

the software automatically checks the inspection code, when the inspection code is in the legal user state, executing of the software is permitted, when the inspection code is in the illegal user state, executing of the software is terminated immediately.

Claim 27. (previously presented) The method of claim 26, wherein when both of he received software serial number and the received communication equipment serial number are not found among the datasets, the software serial number and the communication equipment serial number are written down as a new dataset in the database and then the inspection code is reset to the legal user state.

Claim 28. (original) The method of claim 27, wherein the new product registration center is connected to a software manufacturer system for reporting a registration of software to the software manufacturer system after the new product registration center resets the inspection code to the legal user state according to the software serial number and the communication equipment serial number.

Claim 29. (canceled)

Claim 30. (original) The method of claim 26, wherein the inspection code and the communication equipment serial number of the computer are transmitted to the new product registration center through a network interface.

Claim 31. (original) The method of claim 26, wherein the inspection code and the communication equipment serial number of the computer are transmitted to the new product registration center through a wireless communication network.

Claim 32. (original) The method of claim 26, wherein the inspection code and the communication equipment serial number of the computer are transmitted to the new product

registration center through a global positioning system.

Claim 33. (original) The method of claim 26, wherein the new product registration center is connected to a software manufacturer system for reporting a registration of software to the software manufacturer system after the new product registration center resets the inspection code to the legal user state according to the software serial number and the communication equipment serial number.

Claim 34. (currently amended) A computer system for detecting an illegal loading of a software with a software serial number into the computer system and executing the software thereafter, the computer system comprising:

a microprocessor for generating an inspection code with [[an]] a first value corresponding to a software when the software is installed in the system at the first time and a software serial number of the software is received by the microprocessor, wherein if ~~the inspection code corresponding to the software is not generated~~ the microprocessor is not present, the execution of the software is terminated;

a non-volatile memory coupled to the microprocessor for holding the inspection code; and

a media access controller coupled to the non-volatile memory unit and a communication control interface for transmitting the software serial number of the software and a communication equipment serial number to the new product registration center via the communication control interface, wherein the new product registration center receives the software serial number and the communication equipment serial number and compares the

software serial number and the communication equipment serial number with datasets in a database in the new product registration center, wherein when the software serial number is found within one of the datasets but a communication equipment serial number in the one of the datasets differs from the received communication equipment serial number, the inspection code is reset to [[an]] a second value, wherein the first value indicates the installed software is in a legal user state and the second value indicates the installed software is in an illegal user state,

wherein the software automatically checks the inspection code before executing the software, when the inspection code is in the legal user state, executing of the software is permitted, when the inspection code is in the illegal user state, executing the software is terminated immediately.

Claim 35. (original) The computer system of claim 34, wherein the communication control interface comprises a network interface card.

Claim 36. (original) The computer system of claim 34, wherein the communication control interface comprises a wireless communication network.

Claim 37. (original) The computer system of claim 34, wherein the communication control interface comprises a global positioning system.

Claim 38. (original) The computer system of claim 34, wherein the non-volatile memory unit comprises an erasable programmable read-only-memory.

Claim 39. (original) They computer system of claim 34, wherein the non-volatile memory unit comprises an electrically erasable programmable read-only-memory.

Claim 40. (original) The computer system of claim 34, wherein the memory unit comprises a flash memory.

Claim 41. (currently amended) A software registration center linked to a hardware system for detecting an illegal loading of a software with a software serial number into a computer and executing the software thereafter, wherein the software registration center has a database with a plurality of datasets, when the software registration center receives the software serial number and the communication equipment serial number, the software serial number and the communication equipment serial number are compared with the datasets,

wherein the new product registration center receives the software serial number and the communication equipment serial number and compares the software serial number and the communication equipment serial number with datasets in a database in the new product registration center, wherein when the software serial number is found within one of the datasets while a communication equipment serial number in the one of the datasets is found identical with the received communication equipment serial number, an inspection code is provided with a first value, and when the software serial number is found within one of the datasets but a communication equipment serial number in the one of the datasets differs from the received communication equipment serial number, the inspection code is reset to [[an]] a second value, wherein the first value indicates the installed software is in a legal user state and the second value indicates the installed software is in an illegal user state, wherein

before the computer is able to execute the software, the software automatically checks the inspection code, when the inspection code is in a legal user state, executing of the software is permitted, when the inspection code is in an illegal user state, executing of the software is terminated immediately.

Claim 42. (canceled)

Claim 43. (original) The software registration center of claim 42, wherein the software registration center is connected to a software manufacturer system for reporting an registration of the software to the software manufacturer system after the software registration center resets the inspection code to the legal user state according to the software serial number and the communication equipment serial number.

Claim 44. (canceled)

Claim 45. (original) The software registration center of claim 41, wherein the inspection code and the communication equipment serial number of the computer are transmitted to the software registration center through a network interface.

Claim 46. (original) The software registration center of claim 41, wherein the inspection code and the communication equipment serial number of the computer are transmitted to the software registration center through a wireless communication network.

Claim 47. (original) The software registration center of claim 41, wherein the inspection code and the communication equipment serial number of the computer are transmitted to the

software registration center through a global positioning system.

Claim 48. (original) The software registration center of claim 41, wherein the software registration center is connected to a software manufacturer system for reporting a registration of the software to the software manufacturer system after the software registration center resets the inspection code to the legal user state according to the software serial number and the communication equipment serial number.